UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,358	01/14/2000	Ernst-Michael Hamann	GE-99-008	8276

7590 10/24/2003

James E Murray
69 South Gate Drive
Poughkeepsie, NY 12601

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	5

DATE MAILED: 10/24/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

MRG

Office Action Summary	Application No.	Applicant(s)	
	09/483,358	HAMANN ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 January 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Drawings

1. New corrected drawings are required in this application because of the following reasons: In Figures 5 and 6 no directional arrows are shown to indicate the flow of action taken in the flowcharts; Figure 7 is informal: applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

3. The use of the trademarks IBM, INTEL PENTIUM and MICROSOFT WINDOWS 98 has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 4, and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 1 recites the limitation "one of the several keys" in step a. There is insufficient antecedent basis for this limitation in the claim.

7. Claim 4 recites the limitation "the redundant data elements" in step bb. There is insufficient antecedent basis for this limitation in the claim.

8. Claim 8 recites the limitation "the key" in the preamble. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign 'Certification Practice Statement' version 1.2 (hereinafter VeriSign) in view of Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings), and

Karlton 'Proposal to add attribute certificates to TLS 3.1' (hereinafter Karlton). As per claim 1, VeriSign discloses a method of creating a certificate to certify a key (see VeriSign, 'Certification Practice Statement', version 1.2), wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer of the certificate), the user of the certificate and the key certified by the certificate (see VeriSign, section 2.4.9, Figure 3). The method disclosed by VeriSign is characterized by the following steps:

a) specification of a request for certification of one of several keys by a certification body for a user (see VeriSign, Section 4, 'Certification Application Procedures', especially section 4.2);

b) if in step a) only one key is to be certified, and no basic certificate is yet available for the user, creation of a basic certificate for the user with a defined number of data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body (see VeriSign, Section 4.2, under class 1 type: 'Method of Communicating Application');

c) addition of an identifying characteristic to the basic certificate (see VeriSign, section 2.4.9, Figure 3, serial number);

VeriSign does not teach signing the certificate. However, Stallings teaches that signing messages is a conventional methodology to enable the receiver of the message to verify the origin of the message (see Stallings, page 300, first 3 bullets). More specifically, Stallings teaches that X.509 certificates are conventionally signed to verify that a certificate was generated by a trusted CA (see Stallings, page 342, Figure 11.3,

especially signature data fields). It would be obvious to one of ordinary skill in the art at the time the invention was made for the CA to sign the prototype certificate. The motivation for such an implementation would enable the certificate applicant to verify the CA processing the request. Hence, the method disclosed by VeriSign in view of Stallings further includes the following steps:

d) generation of a digital signature for the basic certificate and addition of the digital signature to the basic certificate (see Stallings, page 342, Figure 11.3, especially signature data fields);

f) generation of a key pair: inherent in the inclusion of a public key data value in the certificate disclosed by VeriSign is the generation of a key pair - public and private keys (see VeriSign, section 2.4.9, Figure 3; see Stallings, page 342, Figure 11.3, subject's public-key info data field).

VeriSign is silent on the matter of a supplementary certificate. However, supplementary certificates have been a major topic among those skilled in the art as it has become well recognized that the X.509 v3 protocol does not meet many of the certificate format requirements that new and emerging secure network transactions require. The X.509 v3 protocol attempted to deal with these concerns with extensions to the basic certificate format; however, these additions did not fully anticipate the growing diversity of network transactions. In light of these concerns, the notion of paired certificates began to establish itself among those skilled in the art: the combined use of an identity certificate (another name that describes the current X.509 certificate), which distinctly identifies the subject of the certificate, and an attribute certificate, which links the subject

with one of a varied number of transaction types, would address the limitations of an X.509 v3 certificate. Karlton discloses an attribute certificate having similar syntax as an X.509 v3 certificate that further extends the use of the identity certificate (see Karlton, page 1, 'What are Attribute Certificates', 'Motivation'; page 2, paragraph 6). He discloses that the attribute certificate augments a basic certificate with additional attribute fields and is associated with the basic certificate by an identifier (see Karlton, page 2, paragraph 7). Finally, since an attribute certificate is a signed object that asserts additional properties of an identity certificate (see Karlton, page 1, 1st paragraph), the attribute certificate also includes a digital signature separate from the one of the basic certificate. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to create a supplementary, signed certificate to augment the basic certificate in the invention disclosed by VeriSign. The motivation for such a combination would enable a standard certificate to take on additional attributes as new traits are found to be desirable without persistently changing the structure of the standard certificate, as disclosed by Karlton (see Karlton, page 1, 1st paragraph, 'Motivation'). Hence, the invention disclosed by VeriSign in view of Stallings and Karlton also includes the following steps:

g) creation of a supplementary certificate for the basic certificate with a key as set out in step f), the identifying characteristic as set out in step c) and additional data fields not registered by the basic certificate (see Karlton, page 1, 1st paragraph; page 2, 'Implementation Outline');

h) generation of a digital signature for the supplementary certificate and addition of the digital signature to the supplementary certificate (see Karlton, page 1, 1st paragraph).

The aforementioned covers claim 1.

11. As per claim 2, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the basic certificate comprises the following data elements: name of certification body, user id of certification body, name of user, user id of user, and identifying characteristic of the basic certificate (see Stallings, page 342, Figure 11.3 (a)).

12. As per claim 3, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the supplementary certificate comprises the following data elements: signature algorithm, validity period of the certificate, extensions, and an identifying characteristic of the basic certificate (see Karlton, page 2, 6th-7th paragraph; see Stallings page 342, Figure 11.3(a) and pages 347-349, 'X.509v3'). VeriSign is silent on the matter of a key and a key serial number being present in the supplementary certificate. However, with the emergence of different key usages (see Stallings, page 348, bullet 'Key Usage'), keys now establish a type of transaction, and as such, they do not solely identify a subject (since now a subject can have multiple keys). Therefore, it would be obvious to one of ordinary skill in the art to store the key data in the supplementary certificate. The

motivation for such an implementation would enable the basic certificate to store information only relevant to the subject and also support the notion of the supplementary certificate as maintaining information relevant to relationships between the subject and other entities (events, organizations, etc.). This motivation is commonly found in the related field of relational databases and can be applied to the public key infrastructure. Furthermore, VeriSign requires that all CAs under the VeriSign PKI retain records for all material events, including key generation, so that an audit trail can be established (see VeriSign, section 3.8 and 3.9). By including a serial number that identifies the key in the supplementary certificate, key identification would be retained (and hence the source of the key generation) within the certificate, and thus establish a convenient reference to the key's history. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the supplementary certificate to store the key serial number. The motivation for such an implementation would promote users trust in the certificate. The aforementioned covers claim 3.

13. As per claim 4, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Stallings discloses that extensions to the X.509 certificate have been incorporated in the third version to categorize key use of the public key in a certificate (see Stallings, page 348-349, 'Key usage', 'Certificate policies', and 'Policy mappings'). Among other reasons, these fields have been incorporated to distinguish the different types of keys for different transaction scenarios (see Stallings, page 348, requirement 5). In the case when a sender

requests multiple key pairs for different types of transactions from a CA, multiple certificates with different key use identifiers would be created to fulfill the requests. In regards to a single certificate that is generated to certify and transport the plurality of keys, Stallings is silent. However, there are many motivations for implementing such an encompassing certificate, including the following: having a certificate that houses all the related keys generated by a CA to a user simplifies the key request. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate a single certificate for several keys attributed to a user. The motivation for such an implementation would enable a more efficient certificate distribution organization. Finally, since a plurality of CAs can define a certificate for a public key (see Stallings, page 342, Figure 11.3(a); page 348-349 'Key and Policy Information'), data elements relevant to each key uniquely distinguishes the type of key and the key generation source (and time) of each key belonging to a user. Hence, the invention disclosed by VeriSign covers the following steps when more than one key with the same validity period is to be certified at one time:

aa) generation of several key pairs (see Stallings, page 348-349, 'Key and Policy Information');

bb) generation of a certificate for several keys with all data elements necessary for the individual keys and keys generated in step aa, omitting the redundant data elements (as disclosed above);

cc) generation of a digital signature for the certificate and addition of the digital signature to the certificate (see Stallings, page 342, Figure 11.3(a), especially Signature data fields).

The aforementioned covers claim 4.

14. As per claim 5, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 4 rejection under 35 U.S.C. 103(a). In addition, the certificate contains the following data elements: name of certification body, user id of certification body, name of user, user id of user, type and version of the certificate, key, validity, serial number, and extensions (see Stallings, page 342, Figure 11.3). Furthermore, inherent in the combination case of obviousness disclosed in the claim 4 rejection, the certificate includes the number and types of keys as data fields.

15. As per claim 6, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the steps of the method disclosed by VeriSign in the event that no basic certificate exists cover the steps defined in claim 6 in the event when a basic certificate already exists. Hence, claim 6 is rejected under VeriSign in view of Stallings and Karlton for the same reasons set forth in the rejection of claim 1.

16. As per claim 7, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 3 and 6 rejections under 35 U.S.C. 103(a). In addition,

the supplementary certificate contains the following data elements: signature algorithm, key, serial number of key, validity period of the certificate, extensions, and identifying characteristic of the basic certificate (see Karlton, page 2, 6th-7th paragraphs; see Stallings page 342, Figure 11.3(a) and pages 347-349, 'X.509 v3').

17. As per claims 8-11, they are method claims corresponding to claims 1-7 and they do not teach or define above the information claimed in claims 1-7. Therefore, claims 8-11 are rejected under VeriSign in view of Stallings and Karlton for the same reasons set forth in the rejections of claims 1-7.

18. As per claim 12, VeriSign discloses a method for creating a certificate for the simultaneous certification of several keys as outlined above in the claim 8 rejection under 35 U.S.C. 103(a). In addition, the key is a public key (see Stallings, page 342, Figure 11.3(a), subjects public-key info).

19. Claims 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign in view of Stallings and Karlton and further in view of Deo et al. U.S. Patent No. 5,721,781 (hereinafter Deo). As per claims 13 and 14, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 4 rejection under 35 U.S.C. 103(a). Although VeriSign is silent on the matter of storing the generated certificates in the non-volatile memory of a smart card, it is conventional in the art for key data to be stored in secured portable devices. For example, Deo discloses an

authentication system where certificates are stored in the ROM of a smart card (see Deo, col. 12, lines 7-22; Figure 2). It would be obvious to one of ordinary skill in the art at the time the invention was made to store the generated certificates in the non-volatile memory of a smart card. Motivation for such a combination would enable the user to mate the benefits of smart card portability and processing capability without compromising the privacy of the key data as disclosed by Deo (see Deo, col. 1, line 55-67).

20. As per claims 15 and 16, VeriSign discloses a method of creating a certificate to certify a key outlined above in the claim 14 rejection under 35 U.S.C. 103(a). In addition, Deo discloses that the certificate is stored/loaded into the RAM of a smart card (see Deo, col. 12, lines 7-22; Figure 2). Hence, the aforementioned covers both claims 15 and 16.

21. As per claims 17 and 18, they are method claims corresponding to claims 14, 15, and 16 and they do not teach or define above the information claimed in claims 14, 15, and 16. Therefore, claims 17 and 18 are rejected under VeriSign in view of Stallings and Karlton and further in view of Deo for the same reasons set forth in the rejections of claims 14, 15, and 16.

22. Claims 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign in view of Stallings and Karlton as applied to claims 1-7 and further in view of

JAVA 'X.509 Certificates and Certificate Revocation Lists' (hereinafter JavaAPI). As per claims 19-25, VeriSign covers a method for creating a certificate to certify a key as outlined above in the claim 1-7 rejections under 35 U.S.C. 103(a). VeriSign is silent on the matter of the method being incorporated into a computer program product on a computer usable medium. JavaAPI discloses a certificate API that can be used to access and manage certificates (see JavaAPI, page 4, java.security.cert package). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement the methods disclosed by VeriSign into a computer program product using the Java API offered by SUN Microsystems. Motivation for such a combination would enable the method disclosed by VeriSign to be implemented into a marketable product. The aforementioned covers claims 19-25.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sudia U.S. Patent No. 5,841,865 discloses an enhanced cryptographic system and method with key escrow feature.

Albanese et al. U.S. Patent No. 6,002,768 discloses a distributed registration and key distribution system and method.

Moses et al. U.S. Patent No. 6,108,788 discloses a certificate management system and method for a communication security system.

Multerer et al. U.S. Patent No. 6,134,658 discloses a multi-server location-independent authentication certificate management system.

Dyksterhouse et al. U.S. Patent No. 6,336,186 discloses a cryptographic system and methodology for creating and managing crypto policy on certificate servers.

Eigeles U.S. Patent No. 6,401,203 discloses a method for automatic handling of certificate and key-based processes.

Carlsson et al. U.S. Patent No. 6,490,367 discloses an arrangement and method for a system for administering certificates.

Kapidzic et al. 'A Certificate Management System: Structure, Functions and Protocols'.

Ellison 'Generalized Certificates' discloses an alternative certificate format.

Rubin et al. 'Interoperability between the X.509 and EDIFACT Public Key Infrastructures: the DEDICA Project'.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jung W Kim
Examiner
Art Unit 2132

Jk
October 7, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100